a communication line connected to said vending device;

at least one host processor connected to said communication line that executes input, output, transmission and reception for executing at least one of vending and refunding of an electronic ticket; and

an electronic ticket storage device, having an interface that electronically connects to said host processor, where said electronic ticket storage device stores electronic money, an electronic ticket, and a transaction history including transactions of electronic money and electronic tickets, and where said transaction history is updated, by a program stored in said electronic ticket storage device, after a transfer of either electronic money or an electronic ticket;

where in response to an electronic ticket purchase request or an electronic ticket refund request, by at least said host processor or said electronic ticket storage device, at least said electronic ticket or said electronic money is sent from said electronic ticket vending device via said communication line.

Applicant and the undersigned attorney gratefully acknowledge the Examiner's courtesy in granting, and during, the telephonic Examiner interview of October 30, 2001. An Interview Summary (PTO-413) mailed October 31, 2001, describes the substance of the interview, and notes that Applicant would herein address certain points maintained by the Examiner during the interview. The remarks below further address these points and also include the reasons for patentability presented by Applicant during the telephonic interview.

In view of the instant Request for Reconsideration, and the Request for Interference filed concurrently with the instant application, Applicant respectfully requests notification indicating the allowability of the pending claims, and declaring an interference with the Hiroya patent.

II. The 35 U.S.C. §112, ¶1 Rejection

The Office Action maintains the rejection of claims 1-11 under 35 U.S.C. §112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. More specifically, the Office Action re-asserts that the written description supports neither the electronic ticket storage device of claims 1, 6, and 11, nor the sending, receiving, and recording of electronic tickets and money as recited in claims 6-10. Additionally, the Office Action (in the "Response to Arguments" section) newly asserts that there is no support for a terminal means separate from the electronic ticket storage means.

Applicant respectfully traverses this rejection, as the application clearly supports each of these claims elements for at least the reasons presented below.

A. The Electronic Ticket Storage Device

In the 07/06/01 Request for Reconsideration, Applicant explained with reference to the following excerpt (hereinafter referenced as "the first excerpt") that the instant application clearly supports an electronic ticket storage device as claimed because the specification clearly and reasonably conveys to an ordinarily skilled artisan that a money module and a trusted agent may be integrated as a discrete component.

> *It may be noted that instead of the trusted agent 120 and money module 6 being embodied as discrete tamper-proof components, they may be fabricated as one tamper-proof module.* In this case, it would not be necessary to establish a secure session for communication between trusted agent 120 and money module 6 in the same transaction device 122. However, discrete money modules 6 and trusted agents 120 are preferable in that such a configuration allows for greater application flexibility. [Emphasis added.]

[Page 35, lines 10-16, (US Patent No. 5,557,518 at col. 20, lines 4-12) (emphasis added).]

In response to Applicant's arguments presented in the 7/6/01 Request for Reconsideration, the Office Action states, in part, the following:

> Applicant's specification describes separate communications between money modules and trusted agents. The description indicates that a fabrication of trusted agent and money module as a single tamper proof module would eliminate the requirement for secure communications between a money module and a trusted agent, <u>but still describes the separate communications between money modules from customer to merchant, and trusted agents from merchant to customer, and separate transaction histories for each</u>. [Emphasis added.]

Concerning this issue of the trusted agent and the money module being integrated as one tamper proof module, the Interview Summary (mailed 10/31/01) states that "Examiner Barron pointed out that integration of the hardware components does not necessarily also support the integration of the functional or logical activities of the elements. In particular, the trusted agent and the money module have separate transaction histories and update programs."

Applicant hereinbelow further elaborates why to an ordinary skilled artisan the specification clearly and reasonably conveys structurally and functionally integrating a money module and an associated trusted agent, thus clearly supporting an electronic ticket storage device as claimed. In elaborating these reasons, Applicant refers not only to the above-cited excerpt, but also to the following (Page36, lines 1-9 ('518 patent col. 20, lines 29-42); hereinafter referred to as "the second excerpt"):

> *In the preferred embodiment, the money module session is established in a manner similar to the establishment of a trusted agent session*. The money modules 6 would therefore hold their own certificates containing their public keys. The swapping of certificates and random numbers (for XORing) enables the secure creation of session keys (MM/MM). The Establish Session protocol used by money modules is shown in FIG. 38 and described subsequently. *The overall system security pertaining to the money modules may be integrated with that for the trusted agents 120, but is preferably separate to provide for enhanced system security and system flexibility*. [Italicized and underlined emphasis added.]

As an initial matter, Applicant respectfully submits that the Office Action's assertion that the specification does not convey functionally integrating the trusted agent and associated money module because the specification "still describes the separate communications between money modules from customer to merchant, and trusted agents from merchant to customer" apparently does not consider this excerpt which expressly describes, as an alternative embodiment, implementing a common communication channel for inter-transaction device communications between money modules and between trusted agents. More specifically, to those skilled in the art, it clearly and reasonably conveys integrating the security functions of a trusted agent and its associated money module such that they may use the *same* certificate (and public key), and thus may communicate over a common communication channel with another transaction device's money module and/or trusted agent. This integrated security and common communication is clearly set forth as an alternative to a trusted agent and its associated money module having separate security, having their own certificates (and public keys), and thus communicating via separate communication channels and necessarily requiring establishing separate communication sessions.

1. "One Module" Clearly Conveys Functionally/Logically Integrating a Trusted Agent and Its Associated Money Module

Referring to the first excerpt, *supra*, Applicant submits that this description of the trusted agent and money module being "*fabricated as one tamper-proof module*" reasonably conveys to those skilled in the art that the trusted agent and money module are fabricated as an integrated *functional* and structural unit (e.g., an integrated hardware and/or software device, such as a program controlled processor, implementing both the trusted agent and money module *functions*).

First, Applicant notes that the specification describes the money module and trusted agent each as *functional* modules, not limited to a specific physical embodiment. For instance, they are each described with reference to their functional components. See, e.g., Figs. 4A-4D and page 15, line 11 et seq. ('518 patent at col. 8, line 55 et seq.); Figure 4 and col. 11, line 37 et seq. of US Patent No. 5,453,601. Indeed, the '601 patent specification states the following:

> [A]ll . . . money modules may be implemented programmatically or by direct electrical connection through customized integrated circuits, or a combination of both, using any of the methods known in the industry for providing the *functions* described . . . [and] [t]hose skilled in the art will appreciate that . . . commercial semiconductor integrated circuit technology would suggest numerous alternatives for actual implementation of the inventive *functions* of the money module that would still be within the scope of the invention. [Col. 10, lines 13-25 (emphasis added).]

In describing transaction money modules, the '601 patent further states (col. 11, lines 33-36) that "[b]ecause the Transaction money module 4 can take on a variety of physical representations, it will be described by the functions performed", and the '601 patent similarly describes other money modules according to their functions. Moreover, the instant application sets forth the protocols implemented by the trusted agent and money module with reference to operational flow charts (e.g., Figures 12-20), again highlighting that the trusted agent and money module are characterized by their functions, and not limited to a specific structural embodiment.

Second, the specification further expressly conveys to those skilled in art that a "module" (e.g., a trusted agent functional unit or money module functional unit) is physically embodied as hardware and/or software (e.g., one or more program controlled processors) designed to carry out the *functions* of that module (e.g., of the trusted agent or money module). For example, the '601 patent explains that "[i]t is contemplated that . . . money modules . . . will be a combination of tamper-proof hardware and application software". '601 patent at col. 8, lines 10-14. Additionally, the instant application states that "[a] trusted agent is a combination of hardware and software components [and] [i]t is tamperproof", thus clearly conveying that a trusted agent is a "module" physically embodied in ways (e.g.., as one or more program controlled processors) similar to money module implementations. Page 6, lines 17-18 ('518 patent at col. 8, lines 9-11).

Accordingly, the explicit description of the trusted agent (i.e., functional module) and its associated money module being fabricated as *one* tamper-proof *"module"* clearly and reasonably conveys that these *functional components* (i.e., modules) may be provided as an integrated functional component (i.e., a module). For example, their respective functions may be logically implemented by a unitary hardware and/or software device (e.g., a processor programmed to execute trusted agent and money module functions). Simply, the disclosure explicitly describes implementing as one functional component (i.e., one module) that which a preferred embodiment describes as being implemented with two functional components (i.e., two distinct modules, namely, trusted agent and money module) that are physically separated.

2. Modifying the Flowcharts of the Disclosed Embodiments in Accordance With the Description Would Result in a Operational Flow Clearly Suited for Implementation as an Device that Physically and Logically/Functionally Integrates a Trusted Agent and Its Associated Money Module

Applicant respectfully submits that the description, including the first excerpt and second excerpt, *supra*, describes modifying the purchase of electronic money protocol (see, col. 17, line 43-col. 23, line 61) in a manner that would result in a process flow that those skilled in the art would clearly and reasonably understand as being a logical/functional integration of trusted agent and money module (and as capable of being implemented, for example, by a common processor executing a program that implements all money module and trusted agent functions).

As Applicant explained in the 7/6/01 Request for Reconsideration, having trusted agent and associated money module functional components embodied in physically separate tamper-proof devices is a preferred—and technically more challenging—way of implementing their functionality that “allows for greater application flexibility” (e.g., it allows trusted agents to be modularly added into any electronic monetary system). Those skilled in the art would understand that the protocols (e.g., purchase of electronic merchandise) described in detail with reference to the flowcharts represent a technically more difficult implementation inasmuch as they describe how to ensure secure communications and transactions (e.g., against the transacting parties and third parties) when a trusted agent functional module and its associated logical money module are implemented in physically separate tamper-proof devices. In the described embodiment, such secure communications are ensured by establishing and using four encryption channels, schematically depicted in the functional block diagram of Figure 13: two (438 and 440) between the respective TAs and MMs, one (436) between the TAs, and one (442) between the MMs.

The ordinarily skilled artisan would further understand that the express description of providing an alternative—and technically much simpler--embodiment (i.e., trusted agent and associated money module functions combined in one tamper-proof component) by (1) *eliminating* (as per the first excerpt) secure sessions for communications between a trusted agent and its associated money module (i.e., eliminating secure channels 438 and 440 in Fig. 13), and (2) *eliminating* (as per the second excerpt) separate secure sessions for inter-trusted agent and inter-money module communications between transaction devices [collapsing 436 and 442 (e.g., eliminating 442) into one common communication channel handling both inter-trusted agent and inter-money module logical messages], may be provided *by simply excising* such security-related steps from the explicitly disclosed process flow that enables physically separate trusted agent and money module, resulting in a process flow that is logically a serial flow (i.e., a serial sequence of trusted agent and money module functional steps). That is, the resulting operational flow is a protocol represented by a sequence of cooperative/interdependent steps/operations effected by trusted agent and associated money module logical entities (e.g., functions, objects, and/or subroutines) without security layers delimiting them, which flow the ordinarily skilled artisan would understand may be implemented in hardware/software on one or more programmed processors to provide a logically/physically integrated trusted agent and money module. Simply, the sequence is *one sequential logical* flow of integrated trusted agent and money module steps, *viz.,* the trusted agent and money module are logically integrated.

In more detail, referring to Figures 16A-16E and the corresponding description in the specification, which describes an anonymous payment protocol and illustrative variations thereof, those skilled in the art would clearly understand that an alternative embodiment in which the secure session between a trusted agent and its associated money module is eliminated (as expressly described by the first excerpt, *supra*, and corresponding to eliminating channels 438 and 440 in Fig. 13) could be provided by *eliminating* (i) steps 520-536 (which involve establishing the secure session), (ii) steps 538-544 involving the sending/receiving of R(1) and R(2) (the random numbers making up the session key); (iii) steps that send messages by encrypting with TA/MM session keys (steps 560, 564, 574, 578, 606, 616, 584, and 586); and steps 548-556 which relate to conveying information for forming the TA/MM session key in the money modules.

In further view of the second excerpt, which clearly and reasonably conveys integrating the overall system security (e.g., involving the management of certificates and session keys) of the trusted agents and money modules, and thus using a common communication channel for inter-transaction device messages logically originating from either a trusted agent or its associated money module, those skilled in the art would further clearly understand that such an embodiment may be provided by eliminating step 546 (eliminating channel 442 in Fig. 13) because this step involves establishing a MM-to-MM session (but an inter-transaction device session has already been established).

Additionally, because the trusted agent/associated money module sessions are eliminated as well as the separate inter-trusted agent and inter-money module sessions (i.e., these communications use a common channel), the ordinarily skilled artisan would clearly understand that the messages designated "E-routed" messages (steps 582, 602, 622, 626, and 632) become regular messages sent over the common secure communication channel used for inter-transaction device communications (used for logically/functionally TA-to-TA messages as well as logically/functionally MM-to-MM messages). [Note, E-routed messages are described as messages using more than one of the session keys MM/MM, TA/MM and TA/TA that are employed in the disclosed embodiment that is suited for physically separate trusted agents and money modules. In that embodiment, inter-money module messages are sent via the trusted agent/associated money module session, and further encrypted by the MM/MM session key and the TA/TA session key. See, e.g., col. 21, lines 43-46.] Further, in view of the foregoing, those skilled in the art would understand that the message protocols represented by Figs. 17-20 would be eliminated.

Applicant respectfully submits that an ordinarily skilled artisan considering this operational flow (and concomitantly, the modified functional block diagram of Fig. 13[1]) that clearly results (note, steps are only eliminated, no additional steps are required) by modifying the disclosed operational flow as described in the specification (and particularly, as per the first and second excerpts) would clearly understand that this resulting operational flow is a logical integration of trusted agent and associated money module functions at least inasmuch as it is a single flow, with message passing between logical components (e.g., trusted agent functions or objects and money module functions or objects), has a common security system for inter-transaction device messages (e.g., logical money module-to-money module messages and/or logical

[1] Applicant notes that the functional block diagram of Figure 13, modified as per the express description set forth in the first and second excerpts, results in a single, common secure communication channel for messages between either TAs or MMs of different transaction devices (with a common certificate for both the TA and MM in a given transaction device) and no secure channel (i.e., 438 and 440) between a trusted agent and its associated money module.

trusted agent-to-trusted agent messages), and has no security provisions for messages between a trusted agent and its associated money module.

3. Additional Remarks Concerning Functional Integration

Applicant additionally notes that even if a program (operating on one or more processors) physically or logically stores electronic money transaction history information in a different format and/or in different steps from electronic ticket information, the program nevertheless updates a transaction history "including transactions of electronic money and electronic tickets", and thus it cannot be said that "the trusted agent and the money module have separate transaction histories and update programs". (Indeed, the Hiroya patent (USP 5,754,654) describes using separate steps for storing the electronic ticket information and the electronic money.)

Applicant further notes that the trusted agent and money module may be considered as being functionally integrated even in the operational flows disclosed for physically separate trusted agent and money module (e.g., Figs. 16A-16E). Particularly, they may be considered functionally integrated at least to the extent that these respective functional components (and their functional sub-components; see, e.g., Fig. 4A for the trusted agent's sub-components) are cooperative and interdependent in effecting a transaction (e.g., anonymous payment protocol); however, they may be considered separate functional modules to the extent that they communicate via security channels implemented because they are in physically separate tamper-proof devices. Thus, fabricating them as one tamper-proof module and eliminating security channels—as the specification expressly describes--may be considered as merely *further* functionally integrating (i.e., to the extent that delimiting security layers are removed) the already functionally integrated trusted agent and money module.

For at least the foregoing reasons, Applicant respectfully submits that the written description clearly supports "an electronic ticket storage device" as claimed, and, moreover, reasonably conveys to those skilled in the art that the disclosed trusted agent and associated money module logical components may be functionally integrated into one tamper-proof module to implement "an electronic ticket storage device [that] . . . stores electronic money, an electronic ticket, and a transaction history including transactions of electronic money and electronic tickets, and where said transaction history is updated, by a program stored in said electronic ticket storage device, after a transfer of either electronic money or an electronic ticket". By way of example, Applicant respectfully submits that a processor executing software that implements all functions of both the trusted agent and the associated money module (which is one illustrative implementation that the description reasonably conveys to those skilled in the art) clearly supports such "an electronic ticket storage device".

B. Sending, Receiving and Recording Electronic Tickets

Applicant notes that while the Office Action's statement of rejection reasserts lack of support for the sending, receiving, and recording of electronic tickets and money as recited in claims 6-10, the Office Action does not provide any response to Applicant's rebuttal arguments that are set forth in the 7/6/01 Request for Reconsideration. Accordingly, Applicant respectfully incorporates by reference and reasserts the arguments presented in that 7/6/01 Request for Reconsideration, and respectfully requests that if the Examiner maintains this basis for the § 112, ¶1 rejection, that the Examiner respond to Applicant's rebuttal arguments.

C. Terminal Means Separate From Electronic Ticket Storage Means

As noted, the "Response to Arguments" section of the Office Action sets forth a new reason for asserting the § 112, ¶ 1 rejection:

> [T]he description of the invention indicates that transaction device, Figure 3, #122, includes three components, host processor, 124, trusted agent 120 and money module 6. While [sic] the invention of the claims requires a terminal means separate from the electronic ticket storage means.

The Interview Summary notes that this new reason was also part of the substance of the interview:

> With respect to the host processor, the examiner pointed out that the claims include a terminal device or means which supports vending that is separate from the electronic ticket storage device, while the Rosen application discloses the host processor as integrated with the trusted agent and the money module.

Applicant respectfully submits that the specification reasonably conveys to those skilled in the art that the host processor and electronic ticket storage device are coupled in a manner such that, for example, they may be physically separable at least inasmuch as the specification shows them coupled or interfaced via a bus (i.e., bus 126), which those skilled in the art clearly understand may include any of myriad types of bus interfaces (e.g., PCI, ISA, PCMCIA, Smart-card) that are well-known to allow the components to be detachable/unpluggable/removable. Thus, the specification does not denote that the transaction device's components must be physically integrated or structurally confined/fixed in some type of physically inseparable local bus architecture.

Further, the Rosen application plainly teaches that a ticket storage device may be interfaced to any one of a number of host devices. For example, as explained in Applicant's interference request submission, the disclosure of U.S. Patent No. 5,453,601 (the '601 patent; which is incorporated by reference into the instant application) describes a preferred money module and host processing device (i.e., the external system or device) to which it is interfaced (page 1, lines 28-30; page 37, lines 6-9), and provides examples of such host processing devices in Figure 3 of the '601 patent as including point of sale (POS) terminals, electronic wallets, personal computers/workstations, mainframes and telephones. See also the related text at Col. 9, line 50 to col. 11, line 36. Accordingly, since the specification describes the ticket storage device as capable of being interfaced to a variety of host devices (e.g., depending on the application), it is clearly intended to be portable (i.e., capable of being ported via a bus interface).

Moreover, as also explained in Applicant's interference request submission, the specification expressly describes the host as providing the communication functions (see, e.g., Page 14, lines 8-13) that allow the ticket storage device to engage in a transaction with another device; therefore, the host is *a fortiori* a terminal, clearly understood by those skilled in the art as being separable from the ticket storage, but interfaced thereto to provide the terminal functions required by the ticket storage device for transacting. [Applicant notes that Hiroya similarly shows that the ticket storage device must be interfaced with a host (terminal means) to effect a transaction.]

Applicant further notes that there is no disclosure expressly requiring the ticket storage device to be permanently and immutably fixed to the host. Therefore, it cannot be said that the Rosen application somehow conveys that the terminal means cannot be separate from a ticket storage device.

Indeed, to the contrary, for at least the reasons explained above, the specification clearly supports a terminal means being separate from an electronic ticket storage means.

Accordingly, for at least the foregoing reasons, Applicant submits that the application reasonably conveys to an ordinarily skilled artisan that at the time of filing Applicant was in possession of the claimed invention. Thus, the rejection of claims 1-11 under 35 USC §112, ¶1 should be withdrawn.

III. <u>Conclusion</u>

In view of the above remarks, Applicant respectfully submits that the application is in condition for allowance. Reconsideration and withdrawal of the outstanding rejections is respectfully requested and allowance of all pending claims is respectfully submitted.

If any outstanding issues remain, or if the Examiner has any suggestions for expediting allowance of this application, the Examiner is invited to contact the undersigned at the telephone number below.

The Examiner's time and attention to this matter are greatly appreciated.

Respectfully submitted,

MORGAN & FINNEGAN, L.L.P.

Dated: January 4, 2002

By: ______________________
David V. Rossi
Registration No. 36,659

CORRESPONDENCE ADDRESS:
MORGAN & FINNEGAN, L.L.P.
345 Park Avenue
New York, New York 10154
(212) 758-4800 Telephone
(212) 751-6849 Facsimile